REMARKS

Claims 1-19 are pending in the current application. In the above amendment, Applicant's representative has corrected a subscript in an equation in a paragraph of the specification of the current application. Because the equation was entered with an equation editor that does not support strikethrough, and because underlining portions of equations can be difficult to interpret, and can be confused with mathematical symbols, Applicant's representative has, in the above amendment, provided the code first in its originally submitted form, and then in a corrected form, rather than using strike-through and underlining.

In an Office Action dated May 2, 2005 ("Office Action"), the Examiner objected to the disclosure because of an incorrect subscript in an equation in the specification of the current application, rejected claims 1-3, 8-12, and 17-19 under 35 U.S.C. § 102(b) as being anticipated by Adams et al., U.S. Patent No. 5,825,886 ("Adams"), rejected claims 4 and 13 under 35 U.S.C. § 103(a) as being unpatentable over Adams in view of Candelore, U.S. Patent No. 5,861,662 ("Candelore"), and rejected claims 5-7 and 14-16 under 35 U.S.C. § 103(a) as being unpatentable over Adams in further view of Menezes et al., NPL Handbook of Applied Cryptography, pages 252-256 ("Menezes"). Applicant's representative has addressed the Examiner's objection to the disclosure, in the above amendment, and wishes to thank the Examiner for a sufficiently careful and comprehensive reading of the disclosure to detect the error in the equation on page 10. Applicant's representative respectfully traverses these 35 U.S.C. § 103(a) rejections.

While Applicant's representative acknowledges that Adams discloses an enhancement to symmetric ciphers that are related to the DES encryption method to which the current claims are directed, and while Applicant's representative very much appreciates an Office Action that cites references related to the general subject matter of the current application, Adams discloses a principle embodiment related to enhancement to CAST ciphers, rather than the Data Encryption Standard ("DES") encryption method to which the current claims are directed, as discussed in greater detail below, and Adams suggests an enhanced DES encryption method different from the DES method described in the current application and claimed in the current claims. Adams' enhancements increase the computational overhead of the encryption

systems by adding additional operations, but gains increased security by doing so. The current claims are directed, by contrast, to an enhancement of the DES method in which a portion of the functionality of the DES expansion permutation step is moved into the DES round key computation function F, in order to improve the computational efficiency of the DES method by decreasing the number of assembly language instructions needed to execute each round of DES computation. Adams' principle embodiment is not a DES method, and does not use either a DES round key computation function F or a DES expansion permutation step. Adams' suggested enhancement to DES does not modify the round key computation function F or the DES expansion permutation step, but, instead, adds an additional operation to each DES computational round. Adams neither teaches, nor discloses, nor mentions, nor in any way suggests Applicant's claimed invention.

Applicant's representative understands that inventors' intent does not, by itself, bear on claim interpretation, but the differences between Adams' disclosed methods and the currently claimed methods arise, in part, both from the differences between the CAST cipher and the DES method as well as from the different goals of Adams' disclosed symmetric cipher enhancement and Applicant's enhancement of the DES encryption system.

Adams' disclosed, principle embodiment relates to an enhancement of CAST ciphers, rather than the DES encryption system. Adams states, in Adams' abstract:

> A new design procedure for constructing a family of DES-like Substitution-Permutation Network (SPN) cryptosystems with desirable cryptographic properties including provable resistance to differential cryptanalysis, linear cryptanalysis, and related-key cryptanalysis is described. New cryptosystems called CAST ciphers, constructed according to the procedure, are also described.

Similarly, in the Field of the Invention section beginning on line 5 of column 1, Adams states:

> The invention resides generally in symmetric cryptosystems and their construction procedures. In particular, it is directed to new ciphers which belong to a family of DES-like substitution-permutation network cryptosystems and to methods of cryptographically transforming plaintext into cipher text using novel ciphers.

Please note that Adams proposes and details enhancement CAST ciphers, and mentions applying a similar enhancement to DES, in order to create encryption systems and ciphers that are less susceptible to cryptanalysis. Adams makes this point again, beginning on line 63 of column 3:

> The design procedure of the invention uses neither of the above approaches. Instead, the invention applies a slight alteration to the typical DES-like round function which renders it "intrinsically immune" (as opposed to computationally immune) to differential and linear cryptanalysis.

By contrast, the current claims a "method of reducing computation during each Data Encryption Standard (DES) encryption and decryption round," a "method of reducing the number of software instructions required to perform permutation and substitution operations using Data Encryption Standard (DES) encryption and decryption rounds," a "method of reducing computation associated with the DES Expansion Permutation by reducing the number of instruction required to compute the inputs to DES SP-boxes," an "apparatus for reducing computation during each Data Encryption Standard (DES) encryption and decryption round," an "apparatus for reducing the number of software instructions required to perform permutation and substitution operations in the Data Encryption Standard (DES) encryption and decryption rounds," and additional, similar methods and devices. *In other words, while Adams seeks to enhance a CAST cipher, similar to, but different from, the DES encryption system, in order to make cryptanalytic attacks directed against the CAST cipher more difficult, the currently claimed methods and systems are directed to making the DES encryption method more computationally efficient.*

Adams explains some of the differences between CAST and DES beginning on line 54 of column 2:

> The CAST design procedure makes use of substitution boxes which have fewer input bits than output bits (e.g., 8 x 32); this is the opposite of DES and many other ciphers which use s-boxes with more input bits than output bits (e.g., 6 x 4).
>
> The design of a good key schedule is a crucial aspect of the cipher design. Keying in the CAST design procedure is done in the manner typical for Feistel networks. That is, an input key (a "primary key") is used to create a number of subkeys according to a specified key scheduling algorithm; the subkey for a given round is input to the round function for use in modifying the input data for that round.
>
> The critical difference between the key schedule proposed in the CAST design procedure and other schedules described in the open literature is the

> dependence upon substitution boxes for the creation of the subkeys. *Other key schedules (the one in DES, for example) typically use a complex bit-selection algorithm to select bits of the primary key for the subkey for round I.* (emphasis added)

Having identified a critical difference between the CAST and DES methods, Adams then discusses the disclosed, principle embodiment, beginning on line 3 of column 6:

> The key schedule used in the embodiment has three main components: *a relatively simple bit-selection algorithm mapping primary key bits to "partial key" bits*; one or more "key transformation" steps; and a set of "key-schedule s-boxes" which are used to create subkeys from partial keys in each round. (emphasis added)

Thus, Adams' disclosed, principle embodiment is not a DES cipher or encryption system. Adams' enhanced CAST cipher does not employ the complex bit-selection algorithm used to select bits for a primary key, while DES does employ a complex bit-selection algorithm. Adams' enhanced CAST system employs substitution boxes, or S-boxes, with fewer input bits than output bits, unlike the DES S-boxes that have a greater number of input bits than output bits, discussed in the current application beginning on line 6 of page 3.

Each of the current, independent, method and systems claims specifically claims a method or system for enhancing the DES encryption system. Adams discloses a principle embodiment comprising an enhanced CAST cipher. Adams clearly states that the CAST cipher differs from the DES encryption system in at least several critical ways. For this reason alone, Adams' disclosed principle embodiment cannot anticipate the currently claimed invention, because Adams' disclosed enhanced CAST cipher is not a DES encryption system, and critically differs from the DES encryption system.

The fact that the CAST system employs or S-boxes with fewer input bits than output bits points to a major difference between Adams' disclosed symmetric cipher enhancements and the currently claimed invention. The CAST system does not need an expansion permutation step, because, in the case of a 32-bit input to a next round of the encryption system, four 8-bit portions of the 32-bit input, following an XOR of the 32-bit input with a subkey, are extracted from the 32-bit input and input to each of four S-boxes, as clearly shown in Figure 2 of Adams, and described in the paragraph beginning on line 23 of column 5. Furthermore, Adams, using

mathematical notation, describes the modification of the CAST round function as $f(R,K)=f(R,K_1,K_2)=S(a(R\oplus K_1,K_2))$, where a is a newly introduced non-linear, key-dependent operation inserted before S-box-table lookup to effectively mask the inputs to the set of S-boxes in order to eliminate the possibility of both differential and linear cryptanalytic attacks against the cipher (Adams, column 6, lines 41-46 and 54). Again, the CAST cipher does not employ expansion and permutation steps, as clearly evident from the lack of encryption and permutation steps in the above round function. CAST does not need to expand the 32-bit input to 48 bits in order to extract 8 6-bit or 4 12-bit inputs to DES 6-bit-input/4-bit-output S-boxes, as described in the paragraph beginning on line 20 of page 2 of the current application. Adams further suggests a similar modification that could be made to the DES encryption system, using similar mathematical notation:

$f(R,K)=S(a(E(R)\oplus K_1,K_2))$ or $f(R,K)=S(a(E(R\oplus K_1),K_2))$

where E is the expansion operation. The newly introduced non-linear, key-dependent operation a is clearly shown to be not a part of the expansion or permutation steps of the DES encryption system, but an operation that follows expansion. In other words, the enhanced CAST cipher is not a DES system, and lacks expansion and permutation steps, and the DES enhancement mentioned by Adams method does not effect or modify the DES expansion and permutation steps.

By contrast, as clearly stated in the Summary of the Invention section of the current application, embodiments of the current invention enable "an implementation of the DES round that requires fewer assembly instructions to complete the existing implementations. The invention furnishes this performance improvement by shifting computation associated with the Expansion Permutation in the DES round to the infrequently executed round key computation function F." This point is stated, in greater detail, in the paragraph beginning on line 7 of page 11 of the current application.

Claim 1 is representative of other independent claims in the current application. Claim 1 is provided below, for the Examiner's convenience, with emphasis added:

1. A method of reducing computation during each Data Encryption Standard (DES) encryption and decryption round, the method comprising the steps of:

a) generating at least one large SP-box lookup table;

b) computing an index for each SP-box lookup table;

c) adding operations to the DES round key computation function to obtain a modified round key computation function; and

d) computing the index for each SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function.

Claim 1 explicitly claims an enhancement to each DES encryption and decryption round in order to reduce computation during each round. Adams, by contrast, increases computation by adding a new operation *a*, as described above, in order to increase security. For this reason, alone, Adams neither anticipates nor makes obvious claim 1, or any other claim of the current claims.

In a first step, a large SP-box lookup table is generated. The CAST-cipher embodiment of Adams does not employ SP-boxes or SP-lookup tables, because the CAST system lacks the permutation step of DES. Adams does not mention SP-boxes when suggesting an enhancement of DES. Not all DES systems employ SP-boxes. For this reason alone, Adams cannot anticipate claim 1, and the other claims of the current claims that all include language directed to SP-boxes and SP-box lookup tables, either explicitly, or through dependence on other claims.

In a final step, claim 1 recites "computing the index for each SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function." The DES encryption system, as explained in the current application beginning on line 20 of page 2, and as clearly shown in Figure 4 of the current application, inputs 32-bit values to an expansion permutation operation that produces a 48-bit output in many DES encryption systems implemented for 32-bit computer architectures. The 48-bit output is then combined in an XOR operation with the output of the DES round key computation function F to produce 8 6-bit or 4 12-bit SP-box-table indexes. The expansion permutation operation, shown in Table 1 on page 4 of the current application, reorders input bits, and includes multiple copies of certain of the input bits in the output, to produce the 48-bit result from a 32-bit input.

Thus, the 48-bit quantity XORed with the DES round key computation function F result is generally not a consecutive set of bits extracted from the 32-bit input. When the bits of the 48-bit output of the expansion step, $y_1 - y_{48}$, are mapped back to the 32-bit input, $x_1 - x_{32}$, computation of one of four 12-bit SP-box indexes is shown, in the lower graphical XOR operation on page 7 of the current application, to involve a set of input bits in which bits x_{12} and x_{13} appear twice, in the bit sequence. A rather large number of assembly instructions are needed to extract and reorder the input bits in this way. Moreover, in the expansion permutation shown in Table 1, both the first 12 bits and the last 12 bits include non-contiguous bits from the original 32-bit input. In the enhanced DES, claimed in claim 1, an embodiment of which is illustrated in the graphical XOR operation shown on page 10 of the current application, a consecutive run of input bits x_8-x_{17} are used as an operand in the XOR operation, saving many assembly language instructions needed to copy and insert copied bits into a sequence of bits specified by the standard DES expansion permutation step. The claimed, enhanced DES moves a portion of the expansion permutation step into the DES round key computation function, for computational efficiency. In the enhanced DES method, each SP-box index can be obtained by XORing a contiguous block of input bits directly with the output of a modified DES round key computation function F.

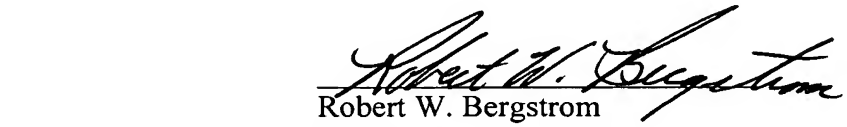
However, as clearly stated in Adams, Adams enhanced CAST cipher does not employ an expansion permutation step, and thus cannot possibly compute an SP-box index using input to an expansion step that has been moved into the DES round key computation function F. CAST does not employ a DES round key computation function F, a critical difference between CAST and DES pointed out by Adams in an above quoted portion of Adams disclosure. As clearly shown in the above discussion, Adams' proposed enhancement to the DES method is a newly inserted operation *a* that follows the expansion permutation step, leaving DES expansion permutation unmodified, and adding to, rather than reducing, the computational overhead of the round computation. The standard DES method does not allow for input bits to be directly input, as contiguous blocks of input bits, to the XOR operation. Thus, Adams' disclosure does not teach, mention, or suggest "computing the index for each SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function." Since a claim is anticipated only if

each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference (MPEP § 2131), the Examiner's 35 U.S.C. § 102(b) rejections of 1-3, 8-12, and 17-19 is unfounded.

The Examiner's 35 U.S.C. § 103(a) rejections of claims 4-7 and 13-16 principally depend on Adams, and fail for reasons similar to those for which Examiner's 35 U.S.C. § 102(b) rejections fail. Adams does not suggest any modification to allow for "computing the index for each SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function." As discussed above, Adams' enhanced CAST cipher does not use an expansion permutation step, and therefore does not allow for computing an SP-box index by XORing input directly with output of a round F function to which expansion-permutation functionality has been moved. Moreover, the CAST cipher does not use a DES round function F, as discussed above. As also discussed above, Adams' proposed enhancement to the DES encryption system introduces an operation *a* that follows the DES expansion permutation step, which outputs a 48-bit quantity representing a reorganized and partially repeated sequence of bits with respect to the input bits. Thus, Adams' proposed DES enhancement does not allow for directly XORing consecutive input bits with a DES round key function F result, since this is not how DES carries out a round of computation. Since Adams neither teaches, mentions, or suggests the claimed enhanced DES method, and the remaining cited references are included only to cover encryption processors and standard DES methodology, and since a *prima facie* case for obviousness can only be established, as stated in MPEP § 2143, citing *In re Vaeck*, when the prior art reference (or references when combined) teach or suggest all the claim limitations, the Examiner has failed to establish a prima facie case of obviousness (see MPEP §2142).

In Applicants' representative's opinion, all of the claims remaining in the application are now clearly allowable. Favorable consideration and a Notice of Allowance are earnestly solicited.

Respectfully submitted,
John Patrick McGregor, Jr.
Olympic Patent Works PLLC



Robert W. Bergstrom
Registration No. 39,906

Enclosures:
Postcards (2)
Extension of Time in duplicate
Transmittal in duplicate

Olympic Patent Works PLLC
P.O. Box 4277
Seattle, WA 98194-0277
206.621.1933 telephone
206.621.5302 fax